USAREUR BULLETIN

Number 10 **HQ USAREUR/7A, Unit 29351, APO AE 09014** **15 May 2000**

This bulletin expires 1 year from date of publication.

ODCSIM REORGANIZATION

The Office of the Deputy Chief of Staff, Information Management (ODCSIM), HQ USAREUR/7A, has reorganized. The division names and office symbols are as follows:

Services Division	AEAIM-SD
Resource Management Division	AEAIM-RMD
Command, Control, Communications, Computer, and Information Technology Division	AEAIM-C4IT
Publishing and Records Management Division	AEAIM-PD

USAREUR Circular 10-10 at *http://www.aeaim.hqusareur.army.mil/library/home.htm* provides information on offices and personnel in each division.

NEW ELECTRONIC REGULATION

The following USAREUR regulation has just been published and is available only in electronic format in the Electronic Library of USAREUR Publications and AE Forms at *http://www.aeaim.hqusareur.army.mil/library/home.htm*:

➢USAREUR Regulation 690-61, Labor-Management Relations—Local National (LN) Employees in Germany, 24 April 2000

NEW USAREUR COMMAND MEMORANDUMS

The following USAREUR command memorandums have been distributed as shown:

➢Month of the Military Child, AEAGA-GY (370-8491), 6 April 2000 (Dist: A)

➢USAREUR Video Teleconferencing Policy, AEAIM-SM-ISB (370-8025), 6 April 2000 (Dist: C)

➢Summer Safety Awareness Campaign 2000, AEAGA-S (370-8084), 25 April 2000 (Dist: C)

➢2000 U.S. Savings Bond Campaign, AEAFC (379-5168), 25 April 2000 (Dist: A)

Units included in the distribution should have received their copies. Proponent telephone numbers are listed after the office symbols. These memorandums are also available in the Electronic Library of USAREUR Publications and AE Forms at *http://www.aeaim.hqusareur.army.mil/library/home.htm.*

DMS IMPLEMENTATION

The Department of the Army will finish the transition from Automatic Digital Network (AUTODIN) service to the Defense Message System (DMS) on 15 June 2000.

Commanders of USAREUR commands (USAREUR Reg 10-5, app A) are responsible for ensuring their organizations are prepared for the DMS transition. 5th Signal Command will coordinate the transition with USAREUR commands.

The POC is Mr. Sanders, DSN 370-8303 or email: sandersb@hq.hqusareur.army.mil.

USAREUR INFORMATION ASSURANCE POLICY

Appendix A provides information assurance policy that applies to users of USAREUR computers and computer networks.

HOW TO USE THIS BULLETIN

HQ USAREUR/7A publishes the USAREUR Bulletin (UB) on the 1st and 15th of each month.

The UB is distributed only by e-mail. Publications clerks who subscribe to the UB will forward each edition of the UB to e-mail accounts in their areas of responsibility.

Other personnel who would like to receive the UB may subscribe to have it delivered directly to their e-mail accounts by sending a request by e-mail to bulletin@upubs.army.mil. The subject line of the e-mail request should be "Subscribe".

Personnel with questions or comments about this bulletin may contact the UB editor by telephone (370-6267) or e-mail (pubsmail@hq.hqusareur.army.mil).

For the Commander:

CHARLES C. CAMPBELL
Major General, GS
Chief of Staff

Official:

JOHN P. CAVANAUGH
Brigadier General, GS
Deputy Chief of Staff,
Information Management

DISTRIBUTION:

This bulletin is distributed by e-mail and is available only in electronic format.

APPENDIX A
USAREUR INFORMATION ASSURANCE POLICY

COMPUTER-NETWORK MISBEHAVIOR

Hacking, possessing hacker tools, or intentionally violating USAREUR policy or regulations on the use of Government computers when using USAREUR computers and networks can—

➢Jeopardize the confidentiality, integrity, availability, and authentication of USAREUR information and information systems.

➢Lead to adverse administrative and judicial action against the violator.

Commanders and supervisors, with help from their information technology and information assurance staff, are responsible for the discipline of USAREUR-computer-network users and operators. The information technology and information assurance staff includes the senior signal staff officer, the information management officer, system and network administrators, and information assurance managers and officers.

LIMITING DAMAGE

Personnel suspected of violating the policy on using USAREUR computers or computer networks will—

➢Be suspended immediately from network access pending the results of a command inquiry.

➢Have their computer accounts inactivated for the duration of the command inquiry. Passwords of which these individuals have knowledge will be changed immediately.

➢Be ordered to not use any USAREUR computer or network pending the results of the command inquiry.

ASSESSING DAMAGE

The Regional Computer Emergency Response Team, Europe (RCERT-E), and the 202d Military Police (MP) Group, United States Army Criminal Investigation Command (USACIDC), will provide technical assistance as required to help commanders assess damage caused by the suspected computer-network misbehavior.

The RCERT-E will—

➢Assess damage that may have resulted from the suspected violator's activities, particularly as they relate to the USAREUR Common User Data Network (CUDN) or the Secure Data Network.

➢Serve as a liaison with the Army Computer Emergency Response Team for finding any damage or harmful activity outside the USAREUR CUDN.

Computer forensic specialists from the 202d MP Group will examine the computer hard drive and other components for evidence of the suspected activity. RCERT-E personnel also will examine RCERT-E computer-activity logs.

PRESERVING EVIDENCE

Computers involved in suspected violations will be removed from the network for examination by computer forensic specialists. These computers will be treated as physical evidence of a crime until released by competent MP authorities.

DETERMINING A COURSE OF ACTION

The unit information technology and information assurance staff, the RCERT-E, and the USACIDC will help the unit commander determine what violations occurred, how they happened, and what damage resulted. The commander will then take the appropriate disciplinary and administrative actions as deemed necessary.

PROHIBITED COMPUTER SOFTWARE

Hacker tools and other unauthorized software applications are not permitted on any USAREUR computer system except as noted below. Units and individuals who have these software applications on their USAREUR computer systems will remove them immediately.

HACKER TOOLS

Hacker tools—

➢Are programs and applications that allow a person to break passwords, gain unauthorized access to someone else's computer system or files, or hide computer activity from auditors or intrusion-detection systems.

➢Include software applications that enable criminal activity, such as generating false computer or personal identities and false credit card numbers.

➢May include normal software applications if these applications are used for other than legitimate purposes.

➢Can identify exploitable vulnerabilities in a computer or network peripheral (server or router) and elevate normal user permission to—

- Give someone unauthorized access to computer resources.

- Allow someone or read, change, or delete information that he or she normally would not be able to read, change, or delete.

Only the following individuals and organizations are permitted to have and use hacker tools and related software applications:

- Officially designated system administrators and network managers while conducting their official missions according to AR 380-19, appendix G, and AR 380-53.

- Law-enforcement and counterintelligence-computer-forensic specialists.

- Computer-threat analysts of the Office of the Deputy Chief of Staff, Intelligence, HQ USAREUR/7A.

- The Regional Computer Emergency Response Team, Europe.

- The Theater Network Operations Center, 5th Signal Command.

OTHER UNAUTHORIZED SOFTWARE

Other software applications that may not be used on USAREUR computer systems include—

- Games.

- Personal software not authorized by the unit information assurance manager.

- Unlicensed (pirated) software.

COMPUTER NETWORK MINIMIZE

Periods of increased military operating tempo (OPTEMPO) place a higher demand on our limited computer network capacity. This demand slows the network, which can affect mission accomplishment.

To ensure the network capacity can support our mission, the Deputy Chief of Staff, Operations (DCSOPS), USAREUR, may issue Network MINIMIZE messages during periods of increased OPTEMPO. These messages will remain in effect until they are rescinded by another DCSOPS message.

Network MINIMIZE applies only to USAREUR-operated Government computers connected to Government networks. When Network MINIMIZE is announced, units must limit their network use, particularly during peak hours of network use (0700 to 1900 Central European Time (CET)).

Examples of measures that may be put in effect during Network MINIMIZE include, but are not limited to—

- Implementing operations-security measures that determine the content of e-mail messages that leave the command.

- Establishing approval authorities for sending e-mail messages outside the command.

- Placing restrictions on—

  - Personal use of computer networks.

  - The size of e-mail messages and attached files.

  - The use of global addresses.

  - The use of mission-related streaming audio and video.

During Network MINIMIZE, mission-essential communications, which include reasonable use of Government computer networks for morale and educational purposes, will be maintained. Personal use of Government computers will not be permitted except for the following:

- Limited morale e-mail by Central Region soldiers, civilian employees, and DOD contractors.

- Limited morale e-mail by soldiers, civilian employees, and DOD contractors forward-deployed to Bosnia and Herzegovina, Kosovo, Macedonia, and other contingency locations.

- Family-support-group use of unit computers to communicate with family members downrange, consistent with the time limits in the above two categories.

- Minimum-essential use of computers at Army education centers for educational purposes. This use will be restricted to off-duty hours. Faculty supervision is requested.

- Minimum-essential use of unit computers for educational purposes. This use will be restricted to off-duty hours and requires supervisory (GS-13, lieutenant colonel, or above) approval.

- Use of Government computers that are not connected to Government networks.

Network MINIMIZE messages will provide provisions for obtaining waivers to network-use restrictions.

ASSIGNING COMPUTER-USER ACCOUNTS TO FOREIGN COALITION FORCES

Among the personnel using USAREUR computers and computer networks are local national employees of, and foreign-national representatives to, the U.S. Government. The policy below applies only to foreign-national representatives to the U.S. Government.

Foreign-national representatives of Allied or Coalition partner countries (both NATO and non-NATO)—

➢May be provided limited-access user accounts on unclassified USAREUR computer networks.

➢Must sign a computer-user agreement before being given an account.

➢May use accounts only for communicating with the U.S. Coalition command structure under which they fall. This use must be consistent with the mission of the Coalition command and with the guidance issued by the U.S. commander responsible for the computer network.

E-mail addresses of foreign-national representatives must include a prefix that identifies the account-holder's country. This prefix must appear before the account-holder's name (for example, uk.smith@tf.army.mil or german.schmidt@tf.army.mil).

User accounts given to foreign-national representatives will fall under the "mnnet.net" domain to protect the worldwide U.S. "dot.mil" domain from access by these individuals.

Access to USAREUR computer networks normally will be restricted to e-mail service and not include Internet access.

➢If a foreign-national representative needs Internet access for a valid military mission, the access requirement must be validated by the Deputy Chief of Staff, Information Management, USAREUR, the Deputy Chief of Staff, Operations, USAREUR, and the USAREUR Information Assurance Program Manager before access is provided. For these representatives, the computer network will be configured to provide only the Internet access required to accomplish the military mission.

➢U.S.-funded Internet access will not be provided to foreign-national representatives for other than official purposes.

The USAREUR policy on the appropriate use of USAREUR computer networks and on limited personal use of U.S. Government computers also applies to foreign-national representatives. Those who misuse USAREUR computer networks will lose access to them, and financial reimbursement for any monetary liability will be requested from the sending country if permitted by applicable international agreements.